The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/05/2013

SUBJECT:
Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEM AFFECTED:

- Google Chrome for Windows, Mac and Linux versions prior to 27.0.1453.110

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Google Chrome. Details of these vulnerabilities are as follows:

- A security vulnerability exists due to a bad handle passed to the renderer. [CVE-2013-2854]
- A memory-corruption vulnerability exists in the dev tools API. [CVE-2013-2855]
- A use-after-free issue in input handling. [CVE-2013-2856]
- A use-after-free issue in image handling. [CVE-2013-2857]
- A use-after-free issue in HTML5 Audio. [CVE-2013-2858]
- A security vulnerability exists due to Cross-origin namespace pollution. [CVE-2013-2859]
- A use-after-free issue in workers accessing database APIs. [CVE-2013-2860]
- A use-after-free issue in SVG. [CVE-2013-2861]
- A memory-corruption vulnerability exists in Skia GPU handling. [CVE-2013-2862]
- A memory-corruption vulnerability exists in SSL socket handling. [CVE-2013-2863]
- A security vulnerability exists due to bad free in PDF viewer. [CVE-2013-2864]
- Multiple unspecified issues affects the application. [CVE-2013-2865]

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/60325

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2854
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2855
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2856
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2857
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2858
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2859
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2860
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2861
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2862
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2863
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2864
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2865

Google:
http://googlechromereleases.blogspot.com/2013/06/stable-channel-update.html